IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Clearview AI, Inc. Consumer Privacy Litigation	)	Case No. 1:21-cv-00135
	)	Judge Sharon Johnson Coleman
	)	Magistrate Judge Maria Valdez

DECLARATION OF THOMAS MULCAIRE IN OPPOSITION TO PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION

I, THOMAS MULCAIRE declare under penalty of perjury pursuant to 28 U.S.C. § 1746 as follows:

1. I have been General Counsel of Clearview AI, Inc. ("Clearview") since September 2019. My duties include planning and executing Clearview's legal and regulatory compliance strategy, handling contractual matters, and managing outside counsel. I am familiar with Clearview's operations, including its information-technology and sales operations. I have personal knowledge of the facts described below, and if called as a witness, I would testify competently thereto.

Clearview's' Operations

2. Clearview is a Delaware corporation with its headquarters and principal place of business in New York.

3. Clearview has no real estate, servers, bank accounts, facilities, or offices in Illinois, and is not registered to do business in Illinois.

4. The servers used in Clearview's business are not in Illinois.

5. Clearview does not sell Clearview's services or app to anyone in Illinois.

6. Clearview does not target Illinois through advertising, marketing, or the use of sales or service representatives.

Clearview's Product

7. Clearview collects publicly-available images on the Internet and organizes them into a database that can be searched remotely by licensed users of the Clearview app.

8. To collect these images, Clearview automatically searches for and downloads the images and associated webpage URLs from the Internet and stores them in a database. Anyone with access to the Internet can obtain the images Clearview downloads to its database.

9. Clearview downloads images from the Internet blindly — that is, without knowing the identities of the people depicted in the images. In some instances, Clearview can determine where a photo was taken based on available metadata, but it impossible for Clearview to determine where the subjects of the images reside. As described further in paragraphs 36-45 below, Clearview has taken a number of technical steps to block Illinois photos from its data collection and search processes, but it cannot determine whether the individuals in the images it does collect from the Internet live in Illinois.

10. When Clearview collects photos from the Internet, the only information Clearview stores from the photos are: (i) the URLs from which the photos were collected; (ii) any metadata associated with the images; and (iii) facial vectors from the faces appearing in the images.

11. Because Clearview cannot determine which individuals depicted in the photos in Clearview's database reside in Illinois, if Clearview were ordered to remove all images of Illinois residents from its database, Clearview would not be able to do so. To comply with such an order, Clearview would likely have to cease using its database altogether. This would effectively shut down Clearview's operations nationwide — even in states that permit Clearview's activities.

12. Clearview does not market, license, or sell products beyond its app that is the focus of this action.

13. When a user searches the app, the user submits a "probe" image, from which

Clearview obtains facial vectors. The facial vectors from the probe are compared to other facial vectors in Clearview's database, and any images associated with close matches to the probe facial vector are returned as search results. Clearview does not add the probe images or the facial vectors derived from the probe images to Clearview's searchable databases of photos or facial vectors.

14. Clearview does not provide the names or facial vectors of any individuals to users of the app. Rather, Clearview provides matching photos and a link to the websites containing those photos.

15. Under no circumstances does Clearview sell, lease, trade, disseminate, disclose, or provide access to any facial vectors to its customers.

16. At no point in using Clearview's app, do any Clearview customers collect, capture, purchase, receive, or obtain any facial vector related to any individual. Clearview's customers are never able to see, access, or control in any way any facial vectors of any individual.

Clearview's Customers

17. Clearview's customers are limited to government agencies, none of which are located in Illinois.

18. As detailed in other declarations submitted in opposition to Plaintiffs' preliminary-injunction motion, Clearview has been instrumental in helping these government agencies solve heinous crimes. Annexed hereto as Exhibit A is a true and correct letter from a law enforcement agency stating that Clearview "has truly been one of the best law enforcement/crime fighting tools our agency has acquired."

19. To take just one example, after the January 2021 riot at the U.S. Capitol, law-enforcement agencies across the country used Clearview's app to identify and investigate several of the suspected perpetrators.

User Agreements

20. Clearview's Servicing Agreement, annexed hereto as Exhibit B, states that Clearview collects photos from the public Internet, performs a scan of facial vectors on certain of the photos, and returns search results to licensed users of its product exclusively as an agent of government agencies.

21. Every customer that uses the Clearview app agrees to the following term of the Servicing Agreement:

> By entering into this agreement with Clearview AI, you expressly authorize Clearview AI to act as an agent on your behalf for the purpose of (i) collecting and compiling publicly available images from the Internet and (ii) producing facial vectors from those images for the purpose of providing the Service to you.

See Exhibit B.

22. Accordingly, Clearview's customers — which are limited to government agencies — have appointed Clearview as their agent for purposes of collecting publicly-available images from the Internet and producing facial vectors from those images. As a result, Clearview acts as the agent of government entities when Clearview collects images from the Internet and produces facial vectors from those images.

23. Clearview's customers can use Clearview's product only for legitimate law-enforcement and investigative purposes. Each customer that uses the Clearview app must be authorized to do so by a government agency.

24. Users may search Clearview's app only if the users enter a case number and crime type, which can be reviewed by that organization's administrative users to ensure that the app is being used appropriately.

Security Measures

25. Clearview has published a policy on its website detailing its retention schedule and

guidelines for permanently destroying biometric identifiers and information. A copy of Clearview's retention policy is annexed hereto as Exhibit C.

26. Clearview has implemented reasonable safeguards to secure its data, including, among other things, (i) a credentialing program to confirm that any licensee of the Clearview app, including a holder of a free-trial license, is who the licensee purports to be; (ii) a system to ensure that any new users of the Clearview app are authorized by their employers to use the app; (iii) dual-factor authentication such that by default, every login session is tied to a proven email address; (iv) encryption of the facial vectors generated by Clearview; (v) the implementation of a bug-bounty program; (vi) the deployment of anti-intrusion devices, such as firewalls and virus scanners; (vii) background checks of employees and contractors; (viii) employee cybersecurity training; (ix) requirements that employees use only electronic devices issued by Clearview for official tasks, and that these devices be accessible to Clearview's information-technology function, which monitors the devices for security threats; (x) blocking access to Clearview's application by IP addresses located in numerous countries, including high-risk countries; and (xi) engaging a third-party audit of the application's code by a cyber-security and risk-management firm to identify and close vulnerabilities.

27. Although Clearview has been the target of sustained cyber threats, to date, none of the photos collected from the Internet by Clearview, facial vectors stored by Clearview, or law-enforcement search histories have ever been compromised.

28. In fact, throughout Clearview's history, there have been only two known instances of unauthorized access of personal information in Clearview's possession. First, in February 2020, an account of a contractor engineer who does not currently work with Clearview was used to access information that included a list of client organizations, the number of accounts they held, and the

number of searches they had performed. Those lists were provided to the media. No facial images collected by Clearview or facial vectors were accessed during the incident. Clearview has addressed the vulnerability that led to this incident.

29. The second incident took place in late March 2020, when an employee of SpiderSilk, a security-research firm, obtained access to an account with limited access on the Clearview Gitlab server. SpiderSilk used this access to exfiltrate information about some Clearview employees, such as Gitlab usernames and an employee email address, as well as certain video files and code associated with Clearview's web application. No facial images collected from the Internet, facial vectors, or other personal information, except the names and emails of two Clearview employees, were accessed during the incident. The vulnerability that led to this incident has been addressed.

30. In addition, Clearview stores the publicly-available photos it downloads from the Internet and corresponding facial vectors separately. Access to these databases is restricted to a small number of Clearview employees with the highest administrative access.

31. No Clearview customers ever have access to Clearview's database of facial vectors.

32. No Clearview customers have access to Clearview's database of publicly-available photos, except for photos appearing in search results.

Clearview's Voluntary Changes to Its Business

33. Beginning in May 2020, Clearview made several voluntary changes to its business practices that are relevant to this litigation.

34. Clearview has cancelled the accounts of every customer that is not a law-enforcement body or a government agency, or their agents or subcontractors. Clearview's terms of use require users agree to use the app only for law-enforcement purposes.

35. Clearview has also cancelled all user accounts belonging to entities located in

Illinois, including law-enforcement bodies and government agencies located in Illinois.

36. Clearview has blocked all photos that have metadata associating them with a geolocation in Illinois (the "Blocked Illinois Photos") from being included in search results on the Clearview app. Although the Blocked Illinois Photos are subject to a document-retention program — which requires the Blocked Illinois Photos to be preserved for ongoing litigation — Blocked Illinois Photos will not appear in any searches on the Clearview app.

37. No Clearview employees can search Clearview's database for the Blocked Illinois Photos, and the limited number of employees with access to the photo and facial-vector databases have signed documentation stating that they understand that Clearview is storing the Blocked Illinois Photos solely for purposes related to ongoing litigation, and stating that they are not permitted to use the Blocked Illinois Photos for any other purpose.

38. Clearview has also included the following language in its user agreements: "[u]sers may not use the Service to research or identify any individuals residing or located in the state of Illinois, U.S.A[.], or the Service within the borders of the state of Illinois."

39. Clearview also blocks login attempts from IP addresses in Illinois to the best of Clearview's ability.

40. Clearview has completed technical modifications to its collection methods to avoid collecting photos of Illinois residents in the future:

a. First, Clearview has constructed a "geofence" around Illinois, meaning that any photo Clearview collects whose metadata bears longitude and latitude data within Illinois is omitted from any data processing.

b. Second, Clearview blocks collection from websites with URLs or page titles containing the terms "Chicago" or "Illinois." Websites hitting on these terms are not processed

into Clearview's database. Likewise, images from websites hitting on these terms are not included in Clearview's search results.

41. Although Clearview cannot exclude with certainty every Illinois resident from its database, Clearview has taken reasonable steps to avoid collecting such images, even if these steps are over-inclusive and will exclude many non-Illinois residents.

42. Clearview has also implemented an opt-out mechanism for any Illinois residents to be removed from Clearview search results. Annexed hereto as Exhibit D is a copy of Clearview's opt-out procedure, which is available on Clearview's website.

43. To exclude a person's photos from Clearview's database and search results, Clearview must first use a photo of the individual to create facial vectors, which are used to ensure that no images of that individual are collected or returned as search results. Because Clearview's app only searches for facial vectors (and does not store any other personal information about an individual in a photo), it would not be technologically possible for Clearview to allow individuals to "opt out" of Clearview's database and search results without creating a facial vector.

44. For this reason, the opt-out procedure requires an individual to provide a photo of him or herself and give consent to the creation of facial vectors that will be used solely to exclude the individual from Clearview's database and search results. Clearview openly discloses that we will generate a facial vector solely to facilitate opt-out.

45. Any facial vectors created for opt-out purposes are subject to strict controls and are used solely for purposes of excluding the individual from the Clearview database and search results.

Clearview's Commitment to Its Business Changes

46. Clearview licenses its product only to government agencies, their agents, and subcontractors, and has procedures to reasonably avoid including photos of Illinois residents in its

database.

47. Although Clearview may develop other products and services in the future, it does not intend to make its app directly accessible to individual consumers.

48. Clearview applied for a patent in August 2019 — before it made the business changes detailed above. On August 7, 2020, Clearview filed a formal application with the patent office that required Clearview to use the same description as the initial application to preserve its intellectual property. Whatever the patent says, Clearview does not intend to make its facial-recognition app available to any individual consumers.

49. To put this issue to bed, Clearview represents to the Court that Clearview will inform the Court and Plaintiffs if, at any point during the pendency of this litigation, Clearview decides to offer products or services to customers who are not law-enforcement agencies or governmental entities or their agents.

Thomas Mulcaire

Dated: Washington, District of Columbia
April 30, 2021

Thomas Mulcaire